STATEMENT OF THE CLAIMS

1 - 42 (previously cancelled)

43 - 62 (cancelled)

63. (new) A method of authenticating data, said method comprising:

(a) storing copies of a plurality of data items;

(b) generating a first data file comprising a respective hash value of each said plurality of stored data items;

(c) generating a single hash value of said first data file derived from said hash values of said plurality of stored data items;

(d) transmitting said single hash value to a remote location, via an information technology communications network;

(e) creating at said remote location a second data file comprising said single hash value and one or more additional data items relating to said single hash value;

(f) generating a hash value for said second data file;

(g) publishing said hash value for said second data file in a dated journal of record published in numerous copies and held in separate public libraries; and

(h) authenticating said second data file by generating a hash value for said second data file and comparing the hash value for the second data file generated in (h) with the hash value for said second data file published in said dated journal.

64. (new) A method according to claim 63, wherein:

said first data file is generated in (b) at the end of a predetermined time period.

65. (new) A method according to claim 64, wherein:

said first data file contains at least one identifier selected from the group consisting of a file name, a path name, a file size and a time stamp.

66. (new) A method according to claim 63, wherein:

least one of said first data items comprises a message to be transmitted from a sender to a receiver.

67. (new) A method according to claim 66, further comprising:

the sender generating a first hash value of said message;

the sender encrypting said message with a first secret key and producing a second hash value from said encrypted message;

the sender encrypting said first secret key with a second secret key;

the sender transmitting to the receiver said encrypted message, said encrypted first secret key and said first hash value;

the sender transmitting said second hash value and said second secret key to a third party;

the third party storing the transmitted second hash value and second secret key for audit purposes;

the receiver receiving said encrypted message and generating a purported copy of said second hash value of said encrypted message;

the receiver transmitting the purported copy of said second hash value to the third party;

the third party determining whether the purported copy matches said second hash value; and

the third party then releasing said second key if a match is so determined.

68. (new) A method according to claim 67, wherein:

the first secret key is symmetric and the second secret key is asymmetric.

69. (new) A method of enabling proof by a third party both of transmission of a message from a sender to a receiver and receipt of said message by said receiver, said method comprising:

the sender generating a first hash value of said message;

the sender encrypting said message with a first secret key and producing a second hash value from said encrypted message;

the sender encrypting said first secret key with a second secret key;

the sender transmitting to the receiver said encrypted message, said encrypted first secret key and said first hash value;

the sender transmitting said second hash value and said second secret key to said third party;

the third party storing the transmitted second hash value and second secret key for audit purposes;

the receiver receiving said encrypted message and generating a purported copy of said second hash value of said encrypted message;

the receiver transmitting the purported copy of said second hash value to the third party;

the third party checking that the purported copy matches said second hash value; and

the third party then releasing said second key if a match is determined.

70. (new) A method according to claim 69, wherein:

the first secret key is symmetric and the second secret key is asymmetric.

71. (new) A method for verifying by a recipient the authenticity of use of an identifier by a sender, said method comprising:

(i) identifying the communication of a message encrypted using a secret key unique to said sender from said sender to said recipient across an information technology communications network;

(ii) accessing, in response to said identification, storage means containing information relating to the most recent message encrypted using said secret key which has occurred across said information technology communications network;

(iii) obtaining confirmation from said sender that said most recent event is valid, and

(iv) preventing further use of said secret key in the event that said confirmation is not received.

72. (new) A method according to claim 71, further comprising:

the sender generating a first hash value of said message;

the sender encrypting said message with said first secret key and producing a second hash value from said encrypted message;

the sender encrypting said first secret key with a second secret key;

the sender transmitting to the recipient said encrypted message, said encrypted first secret key and said first hash value;

the sender transmitting said second hash value and said second secret key to a third party;

the third party storing the transmitted second hash value and second secret key for audit purposes;

the recipient receiving said encrypted message and generating a purported copy of said second hash value of said encrypted message;

the recipient transmitting the purported copy of said second hash value to the third party;

the third party determining whether the purported copy matches said second hash value; and

the third party then releasing said second key if a match is so determined.